Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2014 Proceedings

BUILDING THE NEXT GENERATION OF CYBER SECURITY PROFESSIONALS

Ben Martini
University of South Australia, Adelaide , South Australia, Australia, ben.martini@unisa.edu.au

Kim-Kwang Raymond Choo
University of South Australia, Adelaide, South Australia, Australia, raymond.choo@fulbrightmail.org

Ben Martini and Kim-Kwang Raymond Choo, 2014, "BUILDING THE NEXT GENERATION OF CYBER SECURITY PROFESSIONALS", Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0
http://aisel.aisnet.org/ecis2014/proceedings/track14/3

BUILDING THE NEXT GENERATION OF CYBER SECURITY PROFESSIONALS

Complete Research

Martini, Ben, University of South Australia, Adelaide, Australia, Ben.Martini@unisa.edu.au

Choo, Kim-Kwang Raymond, University of South Australia, Adelaide, Australia, Raymond.Choo@unisa.edu.au

Abstract

Cyber security is an area of strategic and policy interest to governments and enterprises globally, which results in an increase in the demand for cyber security professionals. However, there is a lack of education based on sound theories, standards and practices. In this paper, we adapted the Situational Crime Prevention Theory and the NICE National Cybersecurity Workforce Framework in the design and delivery of our courses, particularly in the Cyber Security Exercise (CSE) which forms an integral part of the courses. The CSE is an attack/defence environment where students are grouped and given a virtual machine with which to host a number of services (e.g. HTTP(S), FTP and SSH) for access by other groups. The CSE is designed to mirror real-world environments where the students' skills will be applied. An overview of the CSE architecture was also provided for readers interested in replicating the exercise in their institutions. Based on student assessment and feedback, we found that our approach was useful in transferring theoretical knowledge to practical skills suitable for the cyber security workforce.

Keywords: Cyber Security Skills; Cyber Security Exercise; National Initiative for Cybersecurity Education (NICE); National Cybersecurity Workforce Framework; Situational Crime Prevention Theory

1 Introduction

Malicious cyber activities are a rapidly expanding form of criminality that knows no borders (Choo 2011; Rudner 2013). To secure our cyber space and protect the confidentiality, availability and integrity of information and communications technologies (ICT), it is essential for cyber security professionals (cyber defenders) to possess up-to-date knowledge, skills, and experiences. Unfortunately, the deficit of a well-developed cyber security workforce complicates recruitment efforts for governments and the private sector to build sophisticated technical cyber capabilities, and has been highlighted as a priority for governments and industries in U.S. (Committee on Professionalizing the Nation's Cybersecurity Workforce 2013) and across the globe.

Educators play an important role in the building of the next generation of cyber security professionals (Paulsen, McDuffie, Newhouse and Toth 2012). To build an effective cyber security workforce, we need to ensure that cyber security education equips students with a holistic perspective on cyber security with an emphasis on proficiency and relevance. Existing information and cyber security curriculum may not necessarily equip students to address complex cyber security problems as our complex cyber threat landscape would 'require [a] learning methodology that produces deeper understanding and critical thinking to defend against increasing[ly] complex cyber attacks' (Dasgupta, Ferebee and Michalewicz 2013, p. 20). A report by the Software Engineering Institute also identified various shortcomings in the traditional classroom training model in building an effective cyber security workforce (Hammerstein and May 2010).

The challenges going forward are increasingly interdisciplinary and multifaceted, all of which will involve knowledge extending across the fields of criminology, law (enforcement), policy, computer science, engineering, et cetera. This is not surprising as cyber security is defined not only by people, process and technical perfection but rather by an ability to manage these imperfections. Engineers and scientists prefer to deal with technical and technological aspects, while humanities and social sciences experts tend to think along strategic and policy lines. Therefore, it is important to reconcile differences in emphasis between the social and technological disciplines in cyber security education. Stockman (2013), for example, demonstrated how social sciences (criminal justice and political science) can be adopted in undergraduate cyber security courses.

To build the next generation of cyber security professionals, we use the Situational Crime Prevention (SCP) Theory (Clarke 1997) as the underlying theoretical lens, and the National Initiative for Cybersecurity Education (NICE)'s National Cybersecurity Workforce Framework (hereafter referred to as NICE Framework – see NICE 2013) as the basis in the delivery of a third-year undergraduate course and a postgraduate cyber security course (may be known as a subject or unit in some universities) at our University. In the next section, we provide a brief overview of the SCP Theory, the NICE Framework, and the delivery of the two cyber security courses. Section 3 outlines the Cyber Security Exercise (CSE), an integral part of the two courses. We also describe how the requirements of the group-based CSE are aligned to a number of NICE Competencies and the SCP Theory. In Section 4, we discuss our findings and conclude the paper in Section 5.

2 Background

2.1 Situational Crime Prevention Theory

The deterrence doctrine (e.g. as the perceived risks and punishments increase, the probability of violations declines) permeates social relations and institutions, and has also been used by information systems researchers studying compliant security behaviour (D'Arcy and Herath 2011). For example, a

review by Siponen, Willison and Baskerville (2008) found that deterrence theory is the single most cited theory in information systems security literature for the period 1990–2004. The general deterrence theory, a utilitarian model that assumes a high degree of rationality, is a theory widely used in the information systems security literature. The theory explains that to reduce ICT violations, individuals must be made aware of an organisation's efforts to curb ICT abuse and of the possibility and/or severity of sanction (Straub 1990). Extrinsic motivators (i.e. increased severity of penalties, increased certainty of detection, and social pressures – normative beliefs) and intrinsic motivators (i.e. perceived effectiveness) can also encourage compliance with organisational information security policies (Herath and Rao 2009a, 2009b).

Another typical response or crime prevention intervention is to create conditions unfavourable to crime, for example, by identifying, manipulating and controlling the situational or environmental factors to limit the opportunities for offenders to engage in criminal behaviour – see SCP Theory (Clarke 1997; Cornish and Clarke 2003). The SCP Theory is a widely used criminology theory in the study of malicious cyber activities. Willison and Siponen (2009), for example, explained how the SCP Theory can be used to reduce employee-related cyber crime. According to the theory:

- criminals are rational decision makers who conduct a cost-benefit analysis prior to offending, and
- most crime is opportunistic, which occurs when a suitable target is in the presence of a motivated offender and is without a capable guardian – see Routine Activity Theory (Cohen and Felson, 1979):

Cornish and Clarke (2003) classified 25 SCP techniques into five broad categories, namely:

(1) Increasing perceived effort: Target hardening, controlling access to facilities, screen exits, deflecting offenders, and controlling tools/ weapons;

(2) Increasing perceived risks: Extending guardianship, assisting natural surveillance, reducing anonymity, utilizing place managers, and strengthening formal surveillance;

(3) Reducing rewards: Concealing targets, removing targets, identifying properties, disrupting markets, and denying benefits;

(4) Removing excuses: Reducing frustrations and stress, avoiding disputes, reducing emotional arousal, neutralizing peer pressure, and discouraging imitation; and

(5) Reducing provocations: Setting rules, posting instructions, alerting conscience, assisting compliance, and controlling drugs and alcohol.

Despite the criticisms against the SCP Theory, there has been 'considerable evidence of the effectiveness of situational crime prevention in reducing crime, both in Australia and overseas' (Morgan, Boxall, Lindeman and Anderson 2013, p. 14). Our findings (see Section 4) also suggested that the SCP Theory and the NICE framework are effective in maximising the outcomes in cyber security courses and preparing students for a cyber security career.

2.2 NICE Framework

To address the human capital crisis in the field of cyber security, the U.S. Government established a Task Force on CyberSkills to identify the best ways of developing a national cyber security workforce and improving the recruitment and retention of cyber security professionals (U.S. Department of Homeland Security 2012). Participants from an ACM Education Board's Workshop on Cybersecurity Education and Training, for example, suggested that the NICE Framework 'is a useful categorization of topics and related skills, and a good starting point from which to build a cybersecurity curriculum' (McGettrick 2013, p. 14).

The NICE Framework comprises 31 specialty areas organized into seven categories. Each specialty area has a list of typical tasks, knowledges, skills, and abilities (KSAs) and competency areas; and we refer interested readers to NICE (2013) for a comprehensive overview of the 31 specialty areas and the associated KSAs due to space constraints.

In the next subsection, we describe the links between 16 of the NICE competency areas and the SCP Theory, and the implementation in our two courses.

2.3 Overview of Courses

Both the third-year undergraduate and postgraduate cyber security courses delivered by the authors at the University of South Australia in 2013 implemented 16 NICE competency areas with the aims of equipping students with the capability to create conditions unfavorable to malicious cyber activities by:

(1) Increasing the perceived effort of the perpetrators (e.g. the use of strong cryptography to secure data-in-transit);

(2) Increasing the perceived risks of being caught (e.g. evidential data uncovered by computer forensics);

(3) Reducing the rewards of malicious cyber activities (e.g. the use of strong encryption to secure data-at-rest);

(4) Removing excuses (e.g. setting of rules and educating students about criminal laws) and

(5) Reducing provocations (e.g. timely patching of software and hardware – see Willison and Siponen (2009)) – see Table 1.

NICE Competencies (Number of KSAs addressed in the courses)	**Situational Crime Prevention Theory**				
	Increase the perceived effort	**Increase the perceived risks**	**Reduce the rewards**	**Remove excuses**	**Reduce provocations**
Information Systems/Network Security (7)	Yes				Yes
Assessment (1)	Yes				
Infrastructure Design (3)	Yes		Yes		
Operating Systems (7)	Yes		Yes		Yes
Encryption (1)	Yes		Yes		
Cryptography (2)	Yes		Yes		
Identity Management (1)	Yes				
Incident Management (4)	Yes	Yes			
Computer Languages (1)					
Configuration Management (2)	Yes				
Computer Network Defense (10)	Yes				Yes
Computer Forensics (1)		Yes			
Information Assurance (3)	Yes	Yes			
Vulnerabilities Assessment (5)	Yes				Yes
Knowledge Management (1)					
Criminal Law (1)				Yes	

Table 1. Applying Situational Crime Prevention Theory to NICE Framework.

Topics covered include network security (e.g. firewalls, intrusion detection and prevention systems, security assessment and testing, network intrusion and countermeasures, and network attacks and countermeasures), cryptography (theoretical asymmetric cryptography, and public key infrastructure and practical implementations of SSL, SSH and VPN), and digital forensics and incident response.

Lectures were delivered over 13 weeks (excluding two weeks of semester break). In addition, students enrolled in the postgraduate course needed to attend a one-week intensive hands-on workshop. The major assessment item for students enrolled in both courses (worth 50% of the overall course grade) was the group-based Cyber Security Exercise (CSE) – see Section 3.

3 Cyber Security Exercise (CSE)

The CSE was a critical component in the process of transferring theoretical knowledge to practical skills useful in the workforce. The weighting of the assessment was significant as to both demonstrate the important of the students' practical understanding of security issues and reward their participation in a time consuming activity over 11 weeks (including the two-week semester break).

The basic premise of the CSE is an attack/defence environment where students are grouped and given a base virtual machine (VM) without an operating system installed but with equal computational resources to the other groups. These VMs must host services for other groups to access. In our version of the CSE, these included a web server (which hosts basic pages and a guestbook web application) with both HTTP and HTTPS services (collectively web services), an FTP server and an SSH server. We selected these services to meet specific educational objectives and Table 2 shows the correlation between the services selected and the key competencies matched in the NICE framework discussed in Section 2.2. While the mixture of services which should be hosted is a topic for debate, we felt that these services were simple and quick to setup and maintain (as this course focuses on security rather than system administration) and yet still deliver the practical skills we sought to convey.

3.1 CSE Design

The 18 postgraduate and 37 undergraduate students were divided into ten groups for the CSE. Each group comprised at least one postgraduate student, one off-campus student and one undergraduate student. Students' participations were assessed on the basis of the following:

- Contribution toward the ongoing activities of the group; and
- Peer review (within the group), where student's contribution is assessed by group members:

  Any student whose peer review mark (within the group) fell below 40% (i.e. less than 2 marks out of a possible 5) had their personal marks for the remaining components of the CSE reduced to a percentage of the group's result determined by their peer review, as a poor peer review indicated that insufficient effort had been made to contribute to the group work. For example,

  - A student scores 30% from their group's peer review (i.e. 1.5 marks out of a possible 5).
  - The group's scores for the report (30%) and presentation (5%) are 25 out of a possible 35.
  - The student who scored 30% during the group's peer review will only receive 7.5 (i.e. 0.3 * 25 = 7.5) out of a possible 35.
- In addition, each group submitted a report, detailing:
  - A summary of their group's activities and decisions, including platform chosen and justification(s).

- Logs of all important "events", such as all attempted attacks on their group's virtual machine and services including time and date, nature of attack, origin of attack, responses taken to prevent/deflect/recover from attack, the damage done, and post-incident assessment.
- Logs of all their group's attempted attacks on other groups including identity of the target, time, date and nature of attack, the source of the idea for the attack, the outcome of the attack, mitigation strategies undertaken by the target (if known), the group's assessment of how well the other group handled the attack, and lessons learnt.
- Logs of their group's attempts to make legitimate use of the services of other machines (e.g. time and date of attempted normal (legitimate) usage, identity of host machine and services requested, response from host – speed/existence of response, and quality of information retrieved).
- Assessment out of 10 (with a brief explanation) for the performance of other groups in the defence of their host and its services.
- A responsibility table that states which group member took final responsibility for each section of the group report. This includes checking for potential plagiarism of content.

After students are introduced to the exercise, they must select their operating system and supporting server applications (e.g. HTTP/HTTPS/FTP/SSH servers, guestbook/anti-malware/firewall/intrusion detection system applications). The students are given between three and four weeks to setup their system and configure the various applications and the selected operating system to be as secure as they deem required. During this time, groups are not allowed to attack each other (and all network communication between groups is prevented via hypervisor software). This is known as the setup phase. Once the setup phase is completed, the production (or attack) phase begins. During the production phase, defence of the groups server is required on a 24/7 basis (naturally this is mostly accomplished by configuration of their operating system and security software's automated responses rather than manual responses).

The following table documents the correlation between NICE competencies (discussed in section 2.3) and services selected for provisioning as part of the CSE.

Service	Key NICE Competencies	Description
Web Services	Information Systems/Network Security Computer Network Defense	Web services have become a predominant facility used by both internal and external users. Securing the various facets (including web server, OS, web applications, CGI environments, etc.) can be a significant part of cyber security professional's responsibilities.
	Infrastructure Design	Providing the students with freedom of choice for web hosting software and web applications gives them the opportunity to experience secure infrastructure design (when conducted in parallel with security theory lectures). Students can experience the effect of errors in their design in a controlled environment.
	Operating Systems	Students have the opportunity to understand the relationship between the OS and their web applications and the security issues in this relationship.
	Encryption/Cryptography	Providing encrypted web services (HTTPS) can be challenging for those without previous experience (especially ensuring a secure configuration is applied). This

Service	Key NICE Competencies	Description
		activity provides this experience in a controlled environment.
	Identity Management	Students were asked to use identity management (user authentication) to protect their guestbook and group specific pages on their web server.
	Vulnerabilities Assessment	Vulnerability assessment was necessary for both ensuring that a group's own web services were secure and for finding flaws in other groups' services.
FTP	Information Systems/Network Security Computer Network Defense	Providing secure file transfer and storage services is an important part of most corporate networks. While FTP is a simple file transfer protocol, it provides students with an understanding of many of the security issues that must be considered when configuring or maintaining a more complex multi user file transfer system.
	Vulnerabilities Assessment	FTP services are subject to a number of vulnerabilities beyond the actual server software itself (which is often quite simple and secure). These vulnerabilities lie with the configuration of the FTP service. This exercise provides students with the opportunity to both exploit the flaws in other groups' services and defend/secure their own service.
SSH	Information Systems/Network Security Computer Network Defense	Remote access is necessary in a modern IT environment both for systems administration and increasingly for user access. Similarly to the other services, remote access (SSH in our environment) is subject to misconfiguration which can have dire consequences especially when privilege escalation is made possible.
	Infrastructure Design Operating Systems	The link between remote access infrastructure and the operating systems being remotely accessed is integral when configuring a secure environment. The default configuration for the majority of SSH servers on both Windows and Linux is not sufficiently secure to resist attacks in a hostile environment. The CSE allows the students to create a configuration suitable for this environment.
	Encryption/Cryptography	The use of encryption and cryptography in SSH is well known and provides for a good practical example of the theories taught in lectures.
	Identity Management	Students made use of identity management when setting up SSH to both authenticate users and grant varied levels of access.
	Vulnerabilities Assessment	As with Web and FTP services vulnerabilities, both the application software and (especially) its configuration can cause vulnerabilities in SSH remote access. This activity gives students the opportunity to locate and see both sides (attacker and defender) of these vulnerabilities.
Core OS	Information Systems/Network Security Computer Network Defense	Apart from vulnerabilities at the application layer, students need to defend their operating systems from attack while finding vulnerabilities in other groups' operating systems. This primarily relates to timely application of security patches but also relates to OS configuration in areas such as

Service	Key NICE Competencies	Description
		application whitelisting and user permissions.
	Infrastructure Design	Providing the students with a choice of operating systems (and operating system variants) adds more complexity to the environment and requires them to consider the underlying decisions made when operating systems are selected in a production environment (e.g. fitness for purpose). This also provides students with a number of potential configurations to attack. For example, some students may use simple identity management systems (e.g. flat file database) while others may use more complex systems (e.g. OpenLDAP or Active Directory) and the students have the opportunity to compare and contrast the advantages and disadvantages from a security perspective.
	Identity Management	Identity management is commonly closely associated with the operating system selected, and configuration of the identity management system is accomplished by OS tools. This exercise provides students with the capability to experiment with multiple types of identity management systems, which would not be possible in a production environment.
	Vulnerabilities Assessment	In addition to application level, vulnerabilities at the OS level can be more complex to find and exploit. However, the rewards for the attacker can often be significant. This exercise provides the students with an opportunity to recognise these types of attacks and defend against them.

Table 2. Correlation between NICE competencies and services defended/attacked.

3.2 CSE Architecture

In the design and development of the CSE (and the two courses generally), we found it important to consider the technical architecture of the CSE. The CSE's importance to the educational outcomes and assessment of the courses caused us to place great importance on ensuring its uninterrupted operation (excepting unavoidable technical constraints). The following are key technical objectives that were defined during the design of the CSE for implementation in the operational version:

- Secure environment – In developing a technical environment for a CSE to be undertaken by students, security of the environment must be considered to be of paramount importance. This is to ensure that the students are not able to accidentally interrupt local (university) or internet hosted resources when conducting attack and defence exercises.

  While a traditional solution to this issue has been to disconnect the environment from the internet (logically or physically), this technique introduced a number of practical issues. These include difficulty using software which requires internet access to download components and, perhaps, most importantly software updates which are integral in a security exercise that runs over several months. For example, it can be quite difficult and tedious to manually update a Windows server without making use of its automatic update facility. We decided that students should focus their time on more productive endeavours and as such sought to provide limited internet access in the environment for purposes such as these.

  In collaboration with our IT services colleagues, we devised a straightforward solution to provide restricted internet access in the environment to a reasonable level of security. This method

involved placing a VPN server in both the CSE virtual local area network (VLAN) and another VLAN, which had direct access to the internet (and specifically not internal systems). Use of this tunnel was restricted to TCP 80 and 443. Session access times were limited to a maximum of 30 minutes per session to discourage keeping the tunnel open, and all traffic was logged to dissuade students from using the tunnel for any purpose other than those specified. 'Split tunnelling' was disabled, which resulted in the students attack/defence VM being disconnected from the CSE VLAN when the internet tunnel was in use.

- Ubiquitous access – Often due to similar security considerations as those discussed above (and also physical hardware availability), cyber security training exercises have been conducted on computers in a single room without the facility for remote access. We sought to leverage the security capabilities of our environment and provide remote access to students to meet their need/desire for flexible working times. This was critical in consideration of the exercise's 24/7 nature and the students' other (study and personal) commitments. It also allowed us to provide a similar experience for the external students enrolled in the courses (who are not required to attend any on campus activities) to the experience provided for the internal students. This had not been possible with previous implementations of this exercise, and we understand it was greatly appreciated by the external students (as reflected in the students' end-of-semester course feedback – also see Section 3.3). It also resulted in some external students being the most productive members of their group in the practical exercise.

  As expected, providing remote access was not without its issues, especially considering the type of access required (i.e. access to an entire VM including virtual hardware as opposed to simply a VNC/RDP session). We understand that the majority of the users received satisfactory performance the majority of the time. However, there are many uncontrollable variables which must be considered when offering this type of capability. These include sufficient remote bandwidth (much more than would be required for a typical remote access session, especially when students attempt to, for example, mount a DVD remotely) and remote client assumptions (e.g. the software client students used to access the environment was only available on Windows. This was an issue as some students used alternative operating systems, although the number of supported operating systems has been improved in newer releases of the environment host software).

- Minimal avoidable downtime – As discussed, the CSE runs on a 24/7 basis which simulates the real-world cyber defence environment. While this provides valuable real world context, for the CSE it also makes the downtime required for maintenance difficult to schedule. Once the exercise commenced, it became obvious that any major changes to the infrastructure hosting the CSE would not be possible. However, to maintain the security principles listed above, ongoing patching of the environment throughout the CSE was critical. Fortunately, most of the components which we used to create the environment were designed with a minimal downtime requirement in mind (as would be required in their usual operation within corporate or cloud datacentres). Hence, the majority of maintenance was possible without disconnecting users. However, some security patches did require the environment hosts to be rebooted. When this was required, the aim was to give the students as much prior notice as possible, sometimes this could be in the order of days, sometimes hours and if the matter was unavoidably urgent minutes. The aim is for the students to stop their work and disconnect gracefully in the time provided. In practice, we found that students made use of the environment at most times of the day.

- Sufficient resources – One of the most frustrating issues for students is system performance. While we were able to provision enough server resources to ensure that performance issues were almost non-existent in terms of the environment host servers, students would often experience latency issues when using remote connections (as discussed above). Anyone wishing to replicate this

exercise should take note of this particular issue and ensure that the system is responsive when being used.

- Equality of resource access – An important consideration throughout the technical design and operation of the environment was ensuring that all participants had equal access to the environments computational resources (as far as possible). This also means ensuring that LAN level exploits are not possible. This consideration is more of a requirement due to the level of assessment associated with the CSE rather than a cyber security requirement (although LAN level attacks such as Address Resolution Protocol (ARP) spoofing – an attack technique where an attacker sends spoofed ARP messages onto a LAN – would not be directly possible for most internet based attackers either).

  Significant technical effort was expended to ensure this aim was met. While the base hosting technologies were able to offer resource control in terms of processing, memory, disk I/O and bandwidth, the host technologies were not able to offer the level of LAN control which was required for our purposes. To meet the needs of this exercise, we employed a third party virtual switch which was able to give us granular control over the traffic flows from each of the VMs and prevent ARP/IP spoofing.

  In addition to the technical measures taken to ensure a level playing field was provided, a number of exercise rules were enforced. These included forbidding a number of attack types such as:

  - IP/MAC/ARP/etc. spoofing – These attacks are difficult (and often impossible) over an internet connection which is the type of defence exercise the CSE is attempting to simulate.
  - Any type of physical attack or social engineering – Physical attacks were excluded and we felt that social engineering had too high a risk of inadvertent damage occurring outside the CSE environment.
  - Extended Denial of Service (DoS) attacks – Extended DoS attacks were forbidden as they are not within the spirit of the exercise and would be somewhat pointless considering all groups have the same level of technical resources.
  - Attacks on the CSE hosting environment.

4 Discussion

Over the 11 weeks that the CSE was operational, the groups conducted and defended against a range of attacks. These include attacks exploiting misconfiguration in systems (e.g. privilege escalation) and identity management (e.g. the use of simple passwords and poor password resetting facility), web application attacks (e.g. SQL injection and cross site scripting attacks), and DoS attacks.

The most common vulnerabilities were due to misconfiguration in systems, and examples include failing to enforce user quotas (e.g. disk spaces, processor time and memory allocation), failing to follow the principle of least privilege (e.g. users having administrative privileges and users having access to applications not required for the exercise) and firewall misconfiguration (e.g. responding to ICMP which resulted in DoS attacks).

Identity management was also commonly exploited in password-based attacks. For example, a number of groups used predictable passwords and one group provided a password reset facility which was exploited by other groups. This was possible as the group only relied on the source IP address being valid. However, the attacking groups found that they could use the web browser available to them as a user on a third group's machine to access the password reset facility.

Web application attacks are a very common internet-based attack, and also an attack of choice by the groups in the CSE. For example, in the Operation Ababil incident reported in Cisco (2013: 56)'s annual security report, it was noted that the attackers 'took advantage of common web applications and hosting servers that are as popular as they are vulnerable'. In the CSE, the groups made use of known vulnerabilities and misconfigurations in existing web applications as well as in custom developed applications for the CSE (e.g. failing to sanitize inputs in a guestbook application resulting in the execution of unauthorized scripts from the web server).

Similar to web application attacks, DoS attacks are an attack of choice by attackers and the groups in the CSE. Examples of DoS attacks attempted in the CSE include depletion of available system resources via scripts using techniques such as Fork bombs (a process that replicates itself to ultimately deplete resources), network flooding (commonly by ICMP), and spamming of guestbooks.

Feedback from the students was positive although students were also of the view that the CSE was very demanding. For example, one group indicated that

> "*[t]he CSE provided an excellent environment for practicing the skills learnt during the tutorials and practical demonstrations (i.e. intensive training week). Our groups' general feeling was that it appears (from the interaction encountered during this practical exercise) to be far harder to defend a webserver than it is to attack.*"

Not surprisingly, most of the students learnt to appreciate the asymmetric nature of cyber security and the importance of a skilled cyber security workforce (i.e. one of the five techniques in "Remove Excuses"). Two groups, for example, commented that:

- "*The CSE was not without its' challenges for all members of group [number removed]. Some have never dealt with either attacking a network or defending a network from attack. Further, not all members of the group had experience in server management, system configuration or the use of other tools such as FTP and SSH. As such the exercise is considered to have been of immense value to all students that have participated ... The diversity amongst the students has provided all students with both courses the ability to investigate offensive and defensive strategies further in the hope that they will all become more competent and aware IT professionals in the future.*"
- "*The Cyber Security Exercise was an excellent tool for learning about the rules and risks of running a publicly accessible service. The largest and most insurmountable obstacle for this group was our lack of previous practical experience with server systems ... Playing a reactionary defensive strategy is less than ideal because a single attack can potentially do irreparable damage. However, it was from these unexpected occurrences that we learned the most, we learned of vulnerabilities that we weren't aware of and ways to exploit weaknesses.*"

Although we did not have the opportunity to formally test the skills of the students before and after the CSE, the students had clearly benefited from the exercise. For example, they were able to articulate the attack and defence strategies used by their group and suggest how the strategies could have been improved in retrospect. This strategic knowledge will, consequently, increase the perceived effort of the attackers against their systems (e.g. using strong encryption and authentication mechanisms) as well as reducing provocations (e.g. regular and timely software patching) and the rewards of malicious cyber activities (e.g. using strong encryption).

Several groups highlighted the importance of prioritizing threats (especially those that could have a damaging effect on the systems) and how the impact of these risks can be reduced if they eventuate at a level considered both acceptable and controllable. The students also understood that it is not always feasible to prevent their systems from being a target (i.e. conceal or remove targets), and to decrease the likelihood of a successful attack, they need to increase the effort and risks required to partake in it. For example, several groups emphasized the importance of existing risk management standards such as Federal Information Processing Standards (FIPS) 199, FIPS 200 and SP 800-53 and best practices

such as National Institute of Standards and Technology's Guide to Enterprise Patch Management Technologies (Souppaya and Scarfone 2013) and the Australian Signals Directorate (2012)'s Top 35 Mitigation Strategies.

- "*We can see the importance of patching both operating system and applications. This was clearly demonstrated with the potentially most damaging event we participated - our root privilege access of Group [number removed] would have been avoided by a simple operating system patch*".
- "*[The CSE themes] fit nicely in the top 4 of the Defence Signal Directorate's [now known as the Australian Signals Directorate] top 4 mitigation strategies, and could be argued are the time honoured "best practice" - patch, whitelist, minimise privilege*".
- "*Allocate users passwords, which include a mixer of alphabetical letter, numeric numbers, and symbol signs if possible. To make hard to be guessed by others … Never trust each user to be able to follow the rules and work within the space, which they have been allowed to work within … Make sure a risk assessment and management is been developed to help assist with security issues that might arise during the setup and production phase*".

5 Conclusion and Future Work

In this paper, we have adapted the SCP Theory and the NICE Framework to provide a useful basis in educating a cyber security workforce. This was demonstrated in our 2013 delivery of a third-year undergraduate course and a postgraduate course. We were able to successfully align a number of NICE competency areas to the SCP Theory, and in turn, match these competency areas to the requirements of the group-based Cyber Security Exercise (CSE). We found that the CSE, in particular, was useful in transferring theoretical knowledge to practical skills suitable for the cyber security workforce. The courses also reinforced the importance of interdisciplinary and cross-domain knowledge (e.g. the importance of ensuring that the methods used in the evidential data collection are in full accordance with applicable laws, legal principles and rules of evidence of the jurisdiction in which the evidence is ultimately to be used). Future work includes extending this approach to other cyber security, digital forensics and related courses at the University, and exploring alternative methods of measuring the practical outcomes of the curriculum (e.g. surveying graduates' employer(s) about their cyber security capabilities over a period of time).

References

Australian Signals Directorate. (2012). Top 35 mitigation strategies. http://www.asd.gov.au/publications/Top_35_Mitigations_2012.pdf

Choo, K.K.R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731

Cisco. (2013). 2013 Cisco annual security report. San Jose, CA, USA: Cisco Systems, Inc.

Clarke, R. (1997). Situational crime prevention: Successful case studies (Vol 2). New York, USA: Harrow and Heston

Cohen, L.E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608

Committee on Professionalizing the Nation's Cybersecurity Workforce. (2013). Professionalizing the nation's cybersecurity workforce? Criteria for decision-making. Washington, D.C., National Academies Press

Cornish, D.B. and Clarke, R.V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention, in Smith, M.J. and Cornish, D.B. (eds), Theory for Practice in Situational Crime Prevention. Crime Prevention Studies no. 16. Monsey, NY: Criminal Justice Press: 41–96

D'Arcy, J. and Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. European Journal of Information Systems, 20(6), 643-658

Dasgupta, D., Ferebee, D.M., and Michalewicz, Z. (2013). Applying puzzle-based learning to cyber-security education. In Proceedings of the Information Security Curriculum Development Conference 2013, pp. 20–26, ACM, Kennesaw, GA, USA.

Hammerstein, J. and May, C. (2010). The CERT® approach to cybersecurity workforce development. Hanscom, MA: Carnegie Mellon University

Herath, T. and Rao, H.R. (2009a). Encouraging information security behavior in organizations: role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165

Herath, T. and Rao, H.R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2):106-125

Hovav, A. and D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Information & Management, 49(2), 99-110

McGettrick, A. (2013). Toward curricular guidelines for cybersecurity: Report of a workshop on cybersecurity education and training. http://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf [Date last accessed: 28 November 2013]

Morgan, A., Boxall, H., Lindeman, K., and Anderson, J. (2013). Effective crime prevention interventions for implementation by local government. Research and Public Policy Series no. 120. Canberra, ACT: Australian Institute of Criminology

Paulsen, C., McDuffie, E., Newhouse, W. and Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. IEEE Security & Privacy, 10(3), 76-79

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. International Journal of Intelligence and CounterIntelligence, 26(3), 453–481

Siponen, M., Willison, R. and Baskerville, R. (2008). Power and practice in information systems security research. In Proceedings of the International Conference on Information Systems, Paris, France, 14-17

Souppaya, M. and Scarfone, K. (2013). Guide to enterprise patch management technologies. Special Publication 800-40 Revision 3, Gaithersburg, MD: National Institute of Standards and Technology

Stockman, M. (2013). Infusing social science into cybersecurity education. In Proceedings of the 14th ACM SIGITE Conference on Information Technology Education, Orlando, FL, USA, 121-124

Straub, D.W. (1990). Effective IS security: an empirical study. Information Systems Research, 1(3): 255-276

U.S. Department of Homeland Security. (2012). Cyberskills task force report Fall 2012. https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf [Date last accessed: 28 November 2013]

U.S. National Initiative for Cybersecurity Education. (NICE). The national cybersecurity workforce framework. http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf [Date last accessed: 28 November 2013]

Willison, R. and Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through Situational Crime Prevention. Communications of the ACM, 52(9), 133-137